09/517,410

## ABSTRACT OF THE DISCLOSURE

A method and apparatus for utilizing a non-secure file server for storing and sharing data securely only among clients and groups authorized to read and modify the data. A first client that desires to store data on the file server encrypts the data with a first encryption key having an associated first decryption key. The client encrypts the first decryption key with a second encryption key having an associated second decryption key known to the first client. Additionally, the first decryption key is encrypted with respective encryption keys of other clients or groups intended to have access to the data stored on the file server and the clients and groups retain their respective decryption keys. All of the encrypted first decryption keys are stored within an access control list in association with the encrypted data on the non-secure file server. In response to an indication that the data should be transmitted to one of the clients, the file server returns to the client the encrypted data along with at least the applicable encrypted first decryption key for the respective client. The client is able to decrypt the first decryption key and decrypt the data using the unencrypted first decryption key. The data may then be modified and securely stored on the file server as described above. The first decryption key may also be encrypted with a second encryption key having a second decryption key known to members of a group or a group server. The first encryption key encrypted with the group second encryption key is stored in the access control list so that group members can obtain access to the encrypted data stored on the file server.

216763



ATTORNEY DOCKET NO. P4421
WEINGARTEN, SCHURGIN,
GAGNEBIN & HAYES, LLP
TEL. (617) 542-2290
FAX. (617) 451-0313